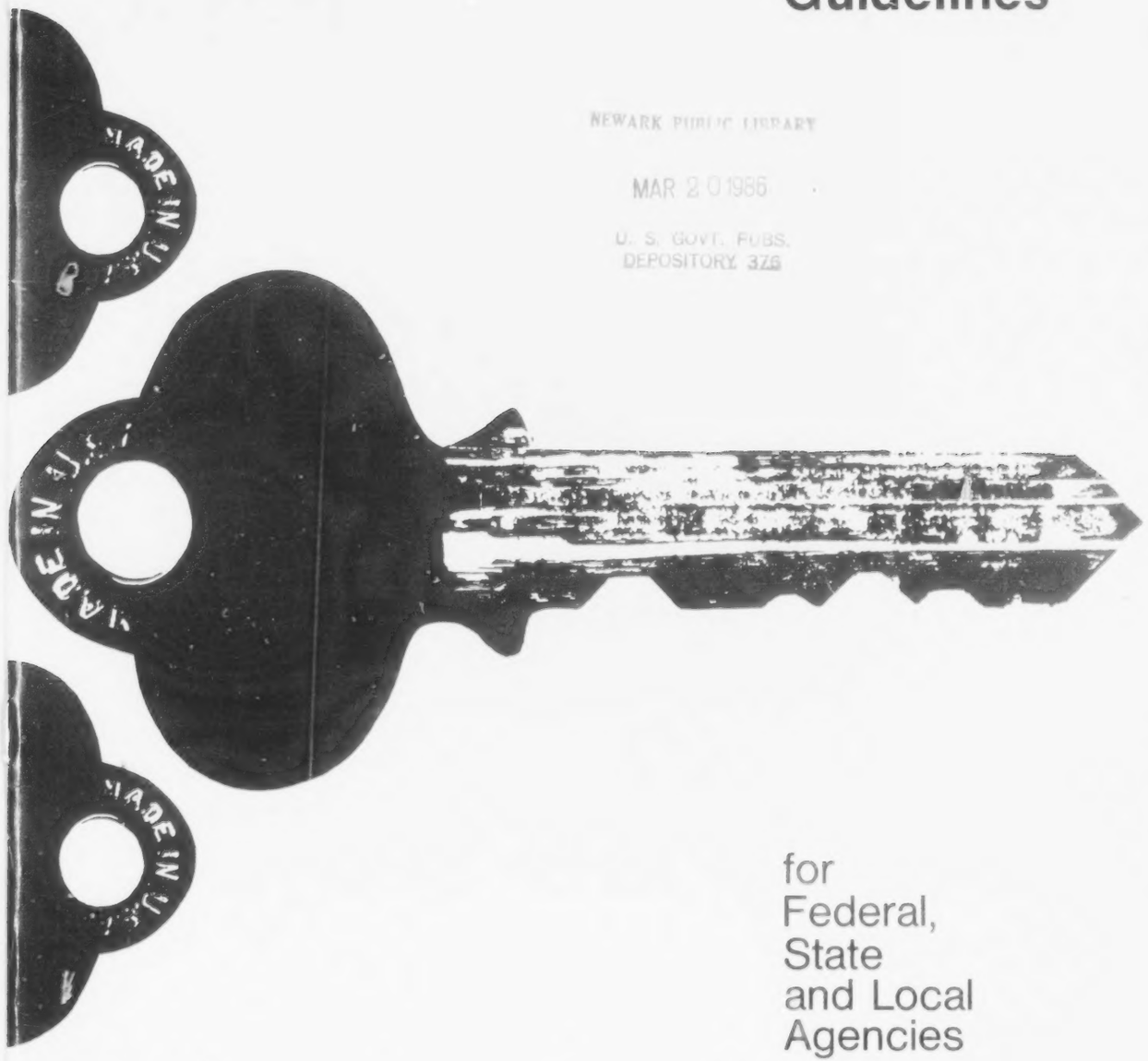
T 19/8/986

Tax Information Security Guidelines

NEWARK PUBLIC LIBRARY

MAR 2 0 1986

U. S. GOVT. PUBS.
DEPOSITORY 325



for
Federal,
State
and Local
Agencies

T 22.19/2:

READEX FICHE best copy available

Contents

I. Introduction/3
II. Requests for Federal Returns and Return Information/3
III. Coordinating Safeguards Within an Agency/4
IV. Internal Inspections/4
V. Recipients Under the Deficit Reduction Act/5
VI. Use of Contractors/6
VII. Reporting Requirements/6
VIII. Employee Awareness/8
IX. Recordkeeping Requirements/8
X. Minimizing Access/9
XI. Use of Return Information in Statistical Reports/11
XII. Control Over Processing/11
XIII. Computer System Security/12
XIV. Security of Storage Areas/13
XV. Methods of Providing Protection/14
XVI. Minimum Protection Standards/16
XVII. Need and Use/20
XVIII. Disposal of Tax Information/21
XIX. Reporting Indications of Improper Disclosure/22
XX. IRS Safeguard Reviews/23

Preface

This publication revises and supersedes Publication 1075 (Rev. 5-85).

I. Introduction

The self-assessment feature is a distinguishing characteristic and principal strength of American tax administration. We in the Internal Revenue Service are acutely aware that in fostering our system of taxation there must be public confidence and trust that we are meeting our legal and moral obligation to protect the confidentiality of personal and financial information furnished to us. Therefore, we must administer the disclosure provisions of the Internal Revenue Code in accordance with the spirit and intent of these laws, ever mindful of this public trust. The Code makes the confidential relationship between the taxpayer and the Internal Revenue Service quite clear. It also stresses the importance of this relationship by making it a crime to violate this confidence. Section 7213 prescribes criminal penalties for Federal and State employees and others who make illegal disclosures of tax information. In addition, section 7431 prescribes civil damages for unauthorized disclosure. The sanctions of the Code are designed to protect the privacy of taxpayers.

Similarly, we recognize the importance of cooperating to the fullest extent permitted by law with other Federal authorities and with State and local authorities in their administration and enforcement of laws. We have strongly supported expansion of programs designed to exchange information with State tax agencies.

The growing concern of citizens and the Congress regarding the individual's rights to privacy, as evidenced both by the frequency of correspondence we receive and the legislation on this subject, makes it doubly important that we reassess our disclosure practices and the safeguards employed to protect the confidential information entrusted to us.

The guidelines contained in this publication pertain not only to those agencies which receive Federal tax information directly from the Internal Revenue Service, but also to those agencies or agents which receive it from secondary sources such as the Social Security Administration and Federal lending agencies.

The guidelines outlined in this publication apply to *all* Federal tax information regardless of the media on which it is recorded. Computerized media containing Federal tax information must be afforded the same levels of protection given to paper documents or any other media with Federal tax information. Security procedures, systemic, procedural, or manual, should preclude circumvention.

A mutual interest exists with respect to our responsibility to insure that tax information is not disclosed to unauthorized persons or used for unauthorized purposes.

We are confident of your diligence in this area. This publication is intended to provide guidance in assuring that the practices, controls and safeguards you employ adequately protect the confidentiality of the data the Service provides to you; we hope you find it helpful. Conformance to these guidelines will meet the safeguard requirements of section 6103(p)(4) of the Internal Revenue Code. Our District Directors have been asked to take a personal interest in the security of tax data. We can jointly benefit by working together in this important area.

II. Requests for Federal Returns and Return Information

Section 6103 of the Internal Revenue Code generally prohibits disclosure of Federal returns and return information. However, exceptions to the general prohibition authorize disclosure of returns and return information to certain Federal, State and local agencies. Generally, these disclosures are made by the IRS in response to written requests signed by the head of the requesting agency. Federal tax information so disclosed may be used by the receiving agency *solely* for the purpose described in the exception authorizing the disclosure.

As a condition of receiving Federal tax returns and return information, the receiving agency must establish and maintain, to the satisfaction of the IRS, certain safeguards designed to prevent unauthorized uses of the information and to protect the confidentiality of that information. In addition to the written request, the IRS may require formal agreements which specify, among other things, how the information will be protected. When an agency makes its initial request, its safeguards should be ready for immediate implementation upon receipt of the information. Copies of the initial and subsequent requests and of any formal agreement should be retained by the agency a minimum of five years as a part of its safeguards recordkeeping system. The recipient agency should submit its Safeguard Procedures Report (See "VII. Reporting Requirements.") when it receives the returns or return information in response to its initial request.

For detailed information concerning requests for Federal returns and return information, you should contact the Disclosure Officer at

the IRS District Office which serves your location or write to:

Director, Disclosure and
Security Division
PM:S:DS
Internal Revenue Service
1111 Constitution Avenue,
NW
Washington, DC 20224

III. Coordinating Safeguards Within an Agency

Because of the diverse purposes for which authorized disclosures may be made to an agency and the division of responsibilities among different, disparate components, and field offices of an agency, Federal returns and return information may be received and used by several quasi-independent units within the agency's organizational structure.

Where there is such a dispersal of returns and return information, the agency should centralize safeguard responsibility and establish and maintain uniform safeguard standards consistent with IRS guidelines. The official assigned these responsibilities should be in a position high enough in the agency's organizational structure to ensure compliance with the agency's safeguard standards and procedures. The selected official should also be responsible for conducting internal inspections, for submitting required safeguard reports to IRS, and for any necessary liaison with IRS.

IV. Internal Inspections

Periodic inspections should be conducted during the year to ascertain that safeguards are adequate. These safeguard inspections should be accomplished pursuant to written procedures which provide for inspection of all local offices by your headquarters. A complete record should be made of each inspection, citing the strong points, as well as deficiencies, and corrective actions taken if appropriate.

The inspection records will be filed in a separate folder, and for purposes of meeting Internal Revenue Code section 6103(p)(4) requirements, will be retained for a period of three years or until reviewed by the Internal Revenue Service.

Safeguard inspections should include the following items:

1. a review of the storage and handling of Federal tax information,
2. a review of how access to Federal tax information is granted to employees,
3. an assessment of facility security features,
4. verification that Federal tax information has not been commingled with other information in such a way that its confidentiality could be inadvertently compromised,
5. a review of after-hours security,
6. a review of access to safes or other secure storage containers or areas and of responsibility for changing keys or combinations as well as the exercise of that responsibility,
7. an analysis of security procedures and instructions to employees,
8. a review of the data processing operations.
9. a review of the control and storage of magnetic tapes,

10. an audit of the file room activity,
11. interviews of those charged with security responsibilities,
12. a review of planned organizational changes to assure that security considerations are covered, and
13. a review of procedures for and records of disposing of or destroying tax information no longer needed by the recipient.

The Tax Reform Act of 1976 provides that safeguards are subject to review by the Internal Revenue Service and the United States General Accounting Office. Your written procedures and inspection findings may be evaluated during these reviews.

The thoroughness and results of your internal inspections will weigh heavily in determining the frequency and extent of the reviews conducted by the Internal Revenue Service.

V. Recipients Under the Deficit Reduction Act

Certain Federal, State, and local agencies may receive return information directly or indirectly, from the IRS and the Social Security Administration (SSA) under specified provisions of the Deficit Reduction Act of 1984 (the Act), codified at 26 U.S.C. 6103(l)(7). The information is provided to the agencies in connection with their administration of certain Federally assisted programs. These agencies must comply with all of the safeguard requirements described in this publication.

Federal agencies receiving return information under the Act will submit their original or modified Safeguard Procedures Reports and their Safeguard Activity Reports to the Director, Disclosure and Security Division PM:S:DS, 1111 Constitution Ave., N.W., Washington, DC 20224. Further, the IRS may assign to certain Federal agencies, with respect to programs they administer, the responsibilities of receiving the Safeguard Procedures Reports and Safeguard Activity Reports of State and local recipients and of monitoring the safeguards established by those State and local agencies. Where a Federal agency is assigned such responsibilities, it shall submit an annual report to the Director, Disclosure and Security Division, describing its safeguard activities, especially whether the agencies are filing timely reports and results of inspections it may conduct, in respect to the State and local agencies for which it has safeguard responsibilities.

State agencies receiving information, whether directly from the IRS or SSA or indirectly through a State coordination agency, under the Act will submit their reports to and be subject to monitoring and on-site inspections by the Federal agency designated in their agreement with the IRS or as otherwise directed by IRS.

Local agencies, below State level, receiving information under the Act will submit their reports to the State agency through which they received the return information for consolidation with that State agency's reports. The local agencies' safeguards are subject to monitoring, including on-site inspections, by the State agency through which they received the return information and by the Federal agency assigned oversight responsibility.

All recipients under the Act are subject to on-site safeguard reviews by IRS.

VI. Use of Contractors

Disclosure of tax returns and return information to contractors is generally prohibited by the tax laws. Two exceptions are disclosures to contractors for tax administration purposes and disclosures to agents of Federal lending agencies for Federal debt collection purposes.

Whenever a contractor is used to process Federal return information the conditions specified in Part XII, "Control over Processing," must be included in the contract. It is the responsibility of the agency which uses the contractor to make certain that all safeguards are in place and utilized by the contractor. IRS may include the contractor's facility in on-site safeguard reviews of the agency.

VII. Reporting Requirements

Safeguard Procedures

In accordance with 26 U.S.C. 6103(p)(4)(E), a written report describing the safeguard procedures established and utilized to assure the confidentiality of Federal tax information will be provided to the Internal Revenue Service at such times as the Service may prescribe. These reports, Safeguard Procedures Reports and Safeguard Activity Reports, are needed by the Service to make its quarterly reports to Congress as required by 26 U.S.C. 6103(p)(5).

The first Safeguard Procedures Report will be submitted within one month after receipt of Federal tax information. (Further Safeguard Procedures Reports will be furnished at the request of the Service.) Federal agencies, and the General Accounting Office should send the report to the Director, Disclosure and Security Division, PM:S:DS, Internal Revenue Service, 1111 Constitution Avenue, N.W., Washington, D.C. 20224. State and local agencies, bodies and commissions should send their reports to the District Director, (Attention: Disclosure Officer) for the district having liaison responsibility. Agents of Federal lending agencies should submit reports directly to their contracting agencies. 26 U.S.C. 6103(l)(7) recipients will report as instructed in Part V.

The report will include the following information:

1. Name, title and telephone number of the official responsible for implementing safeguard procedures;

2. Copies of any statute, portion of a statute or contract governing the agency's functions in pursuance of which the agency, body or commission requests and receives Federal tax returns and return information or, in the case of State tax agencies, copies of the statute or portion of a statute delegating the taxing authority to the agency, body or commission;

3. A chart or description of the agency's organizational structure;

4. A chart or description of the flow of Federal tax data through the organization from its receipt through its return to the Service or its destruction. Pertinent delegation orders or equivalent legal authority which permits use, handling, access, etc., at each point in the flow of tax data should be included;

5. The name and address of other agencies (Federal, State or local) and any officials appointed directly by elected officials who may obtain access to Federal tax returns or return information under the organization's procedures. In connection with this requirement, copies of statutory references, pertinent regulations and copies of interagency agreements reflecting the details of such disclosure will be included. If no such access is allowed under the organization's procedures a statement to this effect will be included;

6. A determination whether Federal tax data is commingled with or transcribed into data kept by the organization;

7. Copies of all other written procedures and other related memoranda concerning the safeguards afforded to the Federal tax information, including a description of the permanent, standardized system of records maintained to record disclosures. These procedures should, at the minimum, describe the physical security afforded Federal tax data, the access allowed to Federal tax data by agency employees, and the manner in which access is controlled. The procedures will also describe in detail the manner in which Federal tax data is disposed of upon completion of use, to include the methods of destruction for different types of data, the place of destruction and time schedule for disposal, and the names or titles of the agency employees who are responsible for supervising destruction or disposal of Federal tax data. The procedures will also describe the agency's security awareness program and the controls used to restrict visitors, janitorial help and unauthorized employees in areas where Federal tax data is maintained. A description of your ADP system capabilities, such as time-sharing, batch processing, or real time access as they relate to Federal tax data (if applicable) including any planned changes or enhancement to your system (equipment, safeguards or programs) and applications of Federal tax data. Also include a brief description of the data processing operations, including system configuration, access controls and audit trail capabilities;

8. Agencies with field offices or subordinate agencies which receive tax returns and tax return information, such as the offices of the United States Attorneys, Department of Justice, are required to include a description of the safeguard procedures established in their field offices or subordinate agencies; and,

9. Copies of written procedures and other memoranda concerning the use of independent contractors in connection with the processing, storage and transmission of Federal tax information, including the use of independent contractors in connection with programming, maintenance, repair, testing, and procurement of data processing equipment used in the processing, transmission and storage of Federal tax data.
See "XII Control Over Processing".

Safeguard Activity Report

Subsequent to submission of the Safeguard Procedures Report, a written Safeguard Activity Report will be submitted annually. This Safeguard Activity Report, which will be signed by the head of the agency or an individual mutually agreed upon by the Service and the agency, will be sent to the same official designated to receive the Safeguard Procedures Report.

The report will:
1. Describe in detail significant changes in safeguard procedures or authorized access to Federal tax returns or return information and any changes or enhancements to physical and computer security measures utilized to safeguard Federal tax data.

2. Describe results of internal inspections conducted by the agency to assure that the written procedures are being adhered to by all agency and contract employees. Included should be the names of offices visited, the specific items reviewed, what the findings were, and the overall safeguard awareness found. Specific items which should be included in the inspection are enumerated in Part IV, "Internal Inspections."

3. Report by general category, the disposal of Federal tax data. The information should be adequate to identify the material destroyed and the date and manner of destruction.

4. In the case of a State tax agency, contain information pertinent to disclosures to State auditors. This will include the name of the individual making the inspection, a description of the records disclosed (including the number of records and the date of the disclosure).

The Safeguard Activity Report serves as your agency's certification that it is protecting return information in accordance with IRC 6103(p)(4).

VIII. Employee Awareness

All agency employees should be thoroughly briefed on all security procedures and instructions requiring their awareness and compliance. Periodic reorientation sessions should be conducted to insure that all appropriate employees remain alert to all security requirements. Consideration should be given to the use of training tools such as: films, audio cassettes, round table discussion, lectures, programmed instruction, and seminars.

Security should periodically be a topic of discussion at managerial meetings. Security briefing sessions should be conducted for supervisors throughout the year. The information presented should be passed on to employees.

There are many ways, in addition to orientations and briefings, that security information and requirements can be brought to the attention of appropriate personnel. For example:

Install security bulletin boards throughout the work areas.

Place security articles in employee newsletters.

Route pertinent articles that appear in the technical or popular press to members of the management staff.

Display posters with short, simple, and educational messages.

Employees must be advised at least annually of the provisions of section 7213(a) of the Internal Revenue Code which makes unauthorized disclosure of Federal returns or return information a crime that may be punishable by $5,000 fine, five years imprisionment, or both. As part of the awareness program, copies of the law must be provided to each employee.

Employees who have access to Federal tax information must also be advised annually of the provisions of section 7431 of the Internal Revenue Code which permits a taxpayer to bring suit for civil damages in a United States district court for unauthorized disclosure of returns and return information. This section allows for punitive damages in case of willful disclosure or gross negligence, as well as the cost of the action. A copy of this law must also be given to each employee.

Employees should be made aware that these civil and criminal penalties apply even if the unauthorized disclosures were made after their employment with the agency terminated.

IX. Recordkeeping Requirements

Federal, State and local agencies, bodies and commissions , and agents authorized under section 6103, which receive Federal tax returns and return information are required by section 6103(p)(4) of the Internal Revenue Code to establish a permanent system of standardized records of requests made by or to them for disclosure of Federal tax returns or return information. The records are to be maintained for five years or the life of the record, whichever is longer.

Magnetic tape files

In the case of magnetic tape files, inventory records must be mantained for purposes of control and accountability. Such records must show the date of receipt, movement and ultimate disposition of the magnetic tapes. In addition, a record count of the number of items on each tape is to be recorded. Any hard copy printout or file resulting from the processing of the tape is to be identified and the disposition of the printout or file should be recorded. Responsible officials must insure that the removal of tapes and discs (containing Federal information) from the storage area is properly recorded on charge-out records. Semiannual magnetic tape inventories should be conducted. All missing tapes must be accounted for. If information generated by a State tax agency after matching State records against IRS magnetic tape reflects more than a recomputed or adjusted State tax liability (such as name, address, SSN, Federal adjusted gross income, etc., which the State previously had no record of) the recordkeeping requirements for other modes of information (as provided below) must also be met for such information.

Information other than that on magnetic tape files

A listing of all documents received from the Internal Revenue Service (including information extracted from magentic tapes) must be maintained by taxpayer name, tax year(s) and type of information (i.e., revenue agent report, Form 1040, workpapers, Criminal Investigation report, etc.) In the case of State and local agencies, reporting requirements must be met only for information which the agency previously did not have in its possession. Such list is to state the reason for and the date each item was requested. In the case of on-going programs, such as the Federal/State exchange agreements, the date would be the date of disclosure by IRS.

In addition, the records must identify the exact location of the Federal data and who has had access to specific Federal data. Chargeout records may be used for this purpose. Information disclosed outside the agency must be recorded on a separate list which reflects to whom the disclosure was made, what was disclosed, and why and when it was disclosed. Tax returns or return information obtained on a specific request basis must be either returned to the IRS, or destroyed after use. However, under certain circumstances, Federal agencies need not return or destroy return information provided safeguards are maintained.

Recordkeeping of disclosures to State Auditors

When disclosures are made by a State tax agency to State Auditors, the above-mentioned requirements pertain only in those instances where the Auditors extract Federal tax information for further scrutiny and inclusion in their work papers.

In those instances where Auditors peruse large volumes of records containing Federal tax information, whether in paper or magnetic tape format, the State tax agency need only identify the bulk records which were examined. This identification will contain the approximate number of taxpayer records, the date of inspection, the best possible description of the records, and the name of the individual making the inspection.

X. Minimizing Access to Federal Tax Information

Federal tax data should be handled in such a manner that it does not become misplaced or available to unauthorized personnel. Good safeguard practice dictates that access to Federal tax information must be strictly on a need-to-know basis. Federal tax data must never be indiscriminately disseminated, even within the recipient Federal or State agency, body or commission. Data needs should be precisely evaluated before Federal tax data is requested or disseminated.

The potential for improper disclosure is minimized by restricting access to designated personnel. The Service recognizes that often it is not feasible to limit access to information to the one individual who received the information. Upon analyzing information furnished by the Service, that individual may determine that certain action is warranted. The official may then forward Federal tax information to technical and clerical employees for necessary processing. However, no person should be given more information than is needed in performance of his/her duties. For example, when documents are given to a clerk/typist, no Federal tax information should be included unless it is needed in performance of clerical or typing duties. Also, when information from a Federal tax return is passed to a technical employee the employee should be provided only that portion of the return that the employee needs to examine.

To avoid inadvertent disclosures to unauthorized persons Federal tax information must be kept separate from other information to the maximum extent possible. State tax agencies should not maintain Federal tax information as part of the administrative file of the State tax return.

In situtations where physical separation is impractical, files should be clearly labeled to indicate that Federal tax information is included and care should be taken to remove all such Federal tax data to preclude access by unauthorized persons.

If Federal tax data is recorded on magnetic media with other data it should be protected as if it were entirely Federal tax data. Such commingling on a single tape should be avoided, if practicable. When data processing equipment is utilized to process Federal tax data, access must be controlled by systemic means if physical or procedural safeguards are limited or inadequate. If your agency shares computer facilities (space, terminals, processor, or memory) with other agencies, departments or individuals who are not authorized to use federal tax data, strict access controls must be maintained which deny access to the Federal tax data. Methods of controlling access will discussed later in this publication.

Access to State tax files by State nontax personnel

Some State disclosure statutes and administrative procedures may permit access by nontax employees. As a general rule, nontax employees are not permitted access to Federal returns and return information under section 6103(d). If you have any questions as to whether particular State employees are entitled to access, your inquiry should be forwarded to the Internal Revenue Service. The Internal Revenue Code clearly provides that Federal tax information shall be furnished to State tax agencies only for tax administration purposes and made available only to designated State tax personnel and legal representatives or to the State audit agency for an audit of the tax agency.

Access to State tax files by political subdivisions of the State

Statutes in several States permit access by political subdivisions such as cities and counties. The Internal Revenue Code does not permit State tax agencies to furnish Federal tax information to a political subdivision for any purpose including tax administration.

Access to State tax files by other States

State disclosure statutes and administrative procedures commonly permit access by other States to tax information. Some States have entered into informal agreements with other States for the reciprocal exchange of tax information. The Internal Revenue Code permits access by State tax officials to Federal tax information pertaining to returns filed by taxpayers residing outside the State upon proper request to the Service. State tax agencies may not furnish Federal tax information to any other State.

Access to State tax files by nongovernmental personnel

Some State statutes may permit nongovernmental access to State tax files under certain circumstances. For example, access might be granted to universities or public interest organizations for research purposes. In such instances, care must be exercised that such persons do not have access to State tax information which has Federal tax information associated with it because universities and public interest organizations cannot have access to Federal returns and return information.

Access to State tax files by other State tax agencies

Some State statutes and administrative procedures may permit access of State tax files by other State tax agencies within the State. However, Federal-State exchange agreements do not permit access by this indirect route.

Each State tax agency desiring Federal tax data must enter into an agreement with the Internal Revenue Service and may not disclose the data received to other State tax agencies (except in special circumstances approved by the Internal Revenue Service).

Charge-out recordation of access

To safeguard the storage of Federal tax information, such information must be charged out when removed from its storage or files area. A written record of the charge-out should be maintained.

The charge-out entry should be dated and include the name, location, and work unit of the employee as well as the reason for the charge-out and a specific description of the materials. Written instructions for accessing the information should be provided including a listing of which employees may be given access to records and also the specific type of records that employees may obtain. The list should be updated as often as necessary.

Provision should be made to assure that access to these records is limited as provided by instructions. A charge-out card should be prepared and inserted in place of the records in the normal filing location.

Responsible officials should review the written charge-out records frequently to ensure the validity of information contained in such records.

XI. Use of Return Information in Statistical Reports

Section 6103 of the Code authorizes the disclosure of Federal returns and return information for use in statistical reports used for tax administration purposes and certain other purposes specified in IRC 6103(j). However, such statistical reports may only be released in a form which cannot be associated with, or otherwise identify, directly or indirectly, a particular taxpayer.

Agencies authorized to produce statistical reports must adhere to the following guidelines or an equivalent alternative which has been approved by the IRS:

1. access to returns and return information must be restricted to authorized personnel;

2. no statistical tabulation may be released with cells containing data from fewer than three returns;

3. statistical tabulations prepared for geographic areas below the State level may not be released with cells containing data from fewer than ten returns; and,

4. tabulations which would pertain to specifically identified taxpayers or which would tend to identify a particular taxpayer, either directly or indirectly, may not be released.

Agencies and organizations seeking statistical information from IRS should make their requests under Internal Revenue Code section 6108(b). The requests should be addressed to:

Assistant Commissioner
(Returns and Information
Processing) D:R:S
Internal Revenue Service
1111 Constitution Avenue, NW
Washington, DC 20224

XII. Control Over Processing

Processing of Federal tax information in magnetic media mode, microfilms, photoimpressions, or other formats (including tape reformatting or reproduction or conversion to punch cards or hard copy printout) shall be performed pursuant to one of the following three procedures:

A. Agency Owned and Operated Facility

Processing under this method will take place in a manner which will protect the confidentiality of the information on the magnetic media. Factors in the Computer System Security section and all other safeguards outlined in this publication must also be followed and will be subject to IRS Safeguard Reviews.

B. An Independent Contractor or Shared-Agency Facility for Tax Administration or Federal Debt Collection.

This method may only be used by an agency which processes Federal tax information for tax administration or Federal debt collection purposes. The following conditions, which should be stated in the contract or agreement, will apply to the use of this method:

1. The contractor or agency-shared computer facility should implement all applicable safeguards outlined in this publication.

2. The contractor or agency shared computer facility is subject to IRS Safeguard Reviews.

3. The contractor or agency shared computer facility must establish written safeguard procedures describing the security measures to be taken to protect the Federal tax data.

4. Only those employees of the contractor or shared computer facility required to process the data under the terms of the contract may have access to Federal tax data; in particular, no State or local agency using the shared facility may have access in any manner to the Federal tax data.

5. The contractor or shared facility should maintain a list of employees authorized access. Such list should be provided to the agency and the IRS reviewing office.

6. The agency must make periodic inspections of the contract or shared computer facility and keep a written record of such inspections.

7. The agency should have the right to void the contract if the contractor fails to provide the safeguards described above.

C. An Independent Contractor or Shared Agency Facility for Recipients under the Deficit Reduction Act

Recipients under the Deficit Reduction Act are allowed to use a contractor or shared facility but only in a manner which does *not* allow access to Federal tax data by the contractor, employees of the contractor, employees of the shared facility, or by any other person or agency not entitled to access under provisions of the Deficit Reduction Act.

The procedures outlined in B above provide reasonable security for tax information. If the contractor or shared agency facility does not employ the conditions contained in B, a statement will be submitted to the IRS subject to review and approval which describes:

Which conditions are not met; and

The action plan for implementing the required conditions that are not present.

The IRS shall *extend* a reasonable period of time for implementation of the required conditions. This grace period shall commence with IRS approval of the action plan.

The above rules also apply to release of magnetic tape to a private contractor or other agency office if the purpose is merely to erase old tapes for reuse.

In conjunction with computer processing of Federal tax data, certain computer operating system conventions must be considered. While Federal tax data is resident in memory, access must be limited to only authorized applications. Also, no Federal tax data should remain on any accessible storage component after the authorized application is completed. If data is retained in some manner, i.e., print file or computer memory, it must be safeguarded in such a way as to prevent unauthorized disclosure. If backup files containing Federal tax data are maintained, whether on-site or off-site, the level of protection must be the same as for the primary files. Whenever maintenance is to be performed on the computer system, all Federal tax data files must be removed to secure storage. If that is not possible, an authorized agency employee must monitor the activities of the customer engineer in order to prevent the unauthorized disclosure of Federal tax data.

A control log or a systemic audit trail must be maintained which records, at a minimum, who accessed the information and when. The log or audit trail should be reviewed periodically to ensure that procedures allow only authorized personnel to access restricted information.

Any computer files created by merging, extracting, or other analysis of Federal data should be labeled and secured the same as the original Federal tax information.

XIV. Security of Storage Areas

When Federal tax data is on computer media, safeguards must be used that will restrict access to those data processing individuals with a need-to-know or, more appropriately, a need-to-process. Authorization codes should be employed (and safeguarded) to ensure access is by authorized persons only. If Federal tax information is accessible through a telecommunications network, security measures must be provided that will make terminals secure either by physical or electronic means to prevent unauthorized use. Authorization codes must be used to protect Federal tax data so that terminal users do not automatically have access to Federal tax data. These authorization codes must be protected, controlled, and periodically changed to ensure that only authorized employees may access the information. When an employee's duties require access to only a portion of the total Federal tax data received, their access should be restricted to that portion.

The return files storage areas require more than normal security. Access to this area should be limited to the absolute minimum number of employees necessary.

The following principles should be followed to adequately restrict access to the files area:

- Written instructions or procedures should be formulated identifying employees who are authorized and those who are not authorized to have access to the tax files.

- Signs should be posted restricting access to the files area

- The location and physical layout of the files area should be such that unnecessary traffic is avoided.

- Any files area containing Federal tax data should be set up and maintained as a secured area.

- Cleaning services should be performed in the presence of an assigned employee:

- Consideration should be given to the use of photo identification cards. The use of a personnel identification system is recommended in all locations where files contain Federal tax data.

- Access to file areas which contain confidential Federal tax information must be restricted to tax administration employees.

- The files area should not contain coffee, lounge or similar facilities which would be used by employees not authorized to have access to Federal tax files.

- Sign-in/sign-out registers should be maintained at each entrance to a restricted area that contains Federal tax files. Each person entering the restricted files area who is not assigned to the area should sign in ink in the register, his/her name, signature, assigned work area, date and time of entry, and purpose of entry. The person controlling the entrance point should verify the name and signature by checking some form of personal identification and enter the time of departure from the area.

- Keys to the files area should be issued only to persons authorized to enter the area.

Security of Magnetic Media

Magnetic tape files should be kept in a secured area under the immediate protection and control of an authorized employee.

Tape reels, disks, or other magnetic media when not in storage, should never be left unattended. When not in use, they should be promptly returned to the storage area.

Good security practice requires that inventory records be maintained for purposes of control and accountability.

Security of Tax Information After Working Hours

During non-duty hours, all areas where Federal tax information is present should be locked. If it is necessary for certain individuals to enter, a procedure should be developed for restricting after-hours access solely to authorized employees.

To the extent practical, Federal tax information in any form (computer printout, photo-copies, tapes, notes, etc.) should be protected after working hours, even if it is in a locked room. Accordingly, such materials should be placed in locked containers when not in use.

General

There are a number of ways that security may be provided for a document, an item, or an area. These include, but are not limited to, locked containers of various types, vaults, locked rooms, locked rooms which have reinforced perimeters, locked buildings, guards, electronic security systems, fences, identification systems and control measures. How the required security is provided depends on the facility, the function of the activity, how the activity is organized and what equipment is available. Proper planning and organization will greatly enhance the security at minimum costs.

Containers

The term container includes all file cabinets, both vertical and lateral, safes, supply cabinets, open and closed shelving or desk and credenza drawers, carts or any other piece of office equipment designed for the storage of files, documents, papers, or equipment.

Some of these containers are designed for storage only, and do not provide protection (for example, open shelving, carts).

For purposes of providing protection, containers can be grouped into three general categories:

1. Security containers
2. Locked containers
3. Safes or vaults

Security Containers

Lockable metal containers approved for the storage of high security items. At present these include the following:

1. Metal lateral key lock files with security modifications.

2. Metal lateral files equipped with lock bars on both sides and secured with combination padlocks meeting FSS Specification FF-P-110.

3. Metal pull drawer cabinets with center or off-center lock bars secured by combination padlocks meeting FSS Specification FF-P-11.

4. Key lock "Mini Safes."

Locked Container

Any wood or metal file, cabinet, desk, credenza or similar type office container which is locked and to which keys and combinations are controlled.

Safes/Vaults

Safes: Safe type containers which have been accepted for general use by the GSA. These can be identified by interior labels which reflect;

1. GSA approval as Class I, II, IV, or V safes; or
2. Safes with TRTL-30, TRTL-60, or TXTL-60, Underwriters Laboratories Listings.

Vaults: Approved vaults are those which have been constructed to GSA specifications and which utilize Underwriters Laboratories approved vault doors.

Rooms and Areas

Restricted Area

A restricted area is an area to which entry is restricted to authorized personnel. All restricted areas should also be secured areas. The use of restricted areas is an effective method of controlling the movement of individuals and eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized disclosure or theft of tax information.

Restricted areas should be prominently identified and separated from non-restricted areas by physical barriers which will control access. The number of entrances should be kept to a minimum, and each entrance controlled. Adequate control should be provided by locating the desk of a supervisor or other responsible employee at the entrance to assure that only authorized persons, with an official need, enter.

A Restricted Area Register should be maintained at the main entrance to the restricted area, and all visitors will be directed to the main entrance. Each person entering the restricted area, who is not assigned to the area, should sign-in by entering in ink in the register: name, signature, assigned work area, person to be contacted, purpose for entry, card number, and time and date of entry. The entry control clerk should identify each visitor by comparing the name and signature entered in the register, with the name and signature of some type of photo identification card, if available. If a photo identification card is not available, identification should be established by the most appropriate means available (e.g., the driver's license). Entry must be approved by the supervisor responsible for the area. When leaving the area, the employee should enter the departure time in the register.

Each Restricted Area Register should be closed out at the end of each month, and reviewed by the restricted area supervisor. It is recommended that the register be reviewed by a second level of management. Each review should determine the need for access for each individual.

To facilitate the entry of employees who have a frequent and continuing need to enter a restricted area, an Authorized Access List can be maintained. Individuals whose names appear on the Authorized Access List, should not be required to sign-in, and the control clerk should not be required to make any entry in the Restricted Area Register. If there is any doubt as to the identity of the individual prior to permitting entry, the entry control clerk should ensure, to his/her satisfaction, the identity of the individual prior to permitting entry. The Authorized Access List will be prepared, dated, and approved by the restricted area supervisor. A new list should be prepared for each month.

Secured Area

A secured area is an area that prevents undetected entry when not occupied by regularly assigned employees.

For purposes of providing protection, all space can be classified as either secured or non-secured.

XVI. Minimum Protection Standards (MPS)

Secured areas are perimeter and/or internal areas which have been designed to prevent undetected entry by unauthorized persons during non-duty hours. To qualify as a secured area, space must meet the following minimum standards:

1. Space must be enclosed by:

- Slab-to-slab walls constructed of approved materials and supplemented by periodic inspection or other approved protection methods; or

- Any lesser type partition (floor to ceiling walls are required for IRS perimeters) supplemented by Underwriters Laboratories approved electronic intrusion detection and fire detection systems.

2. Unless electronic intrusion detection devices are utilized, all doors entering the space must be locked, and strict key or combination control should be exercised.

Space which does not meet the above criteria, cannot be considered as a secured area, since it does not provide adequate security for protected items.

The Minimum Protection Standards (MPS) system is the method utilized by the Internal Revenue Service to provide basic safeguards for documents and facilities. Federal and State agencies should use this illustration of the MPS system as a guide for providing comparable safeguards for tax returns or return information in their possession. Federal and State agencies are not required to use exactly the same methods that the Internal Revenue Service utilizes. Agencies are required to have comparable safeguards for the protection of tax data.

The Minimum Protection Standards (MPS) system establishes a uniform method of protecting data and items which require safeguarding. This system contains minimum standards which will be applied on a case-by-case basis. Since local factors may require additional security measures, management must analyze local circumstances to determine space, container, and other security needs at individual facilities. The MPS has been designed to provide management with a basic framework of minimum security requirements which will provide greater flexibility in dealing with local conditions.

The following describes the MPS and the concepts of protectability using the MPS.

Protected Items/Data

Items and data to be protected are divided into three groups:

1. *Special Protection*—Items which require a specific type of containerization, regardless of the area security provided, due to special access control needs. This group of items is divided into three levels:

- Level 1 (SP-1)—requires storage in a safe or vault;

- Level 2 (SP-2)—requires storage in a security container;

- Level 3 (SP-3)—requires storage in a locked container.

Examples of items designated as special protection are:

SP-1 Classified information—Secret/Top Secret
SP-2 Classified Information—Confidential
SP-1 Combination Records—Forms 4032—safes and vaults
SP-2 Combination Records—Forms 4032 for container or doors
SP-3 Annual Listing of Undelivered Refund Checks
SP-2 Grand Jury—Case files and information
SP-2 Passwords and Password Registers
SP-2 Informant Communications File
SP-2 Informants Claims for Reward
SP-2 Informants Control File
SP-3 Internal Audit/Internal Security Report
SP-3 Key—to any locked container
SP-2 Key—to any room, area, secured area, or security container
SP-2 Limited Official Use Documents

2. *High Security*—Items which require greater than normal security, due to their sensitivity and/or the potential impact of their loss or disclosure. Examples of items designated as high securtiy are:

- Legal Case Files.

- Magnetic Media—all discs, tapes or similiar media which contain program, taxpayer, or other individual data.

• Disclosure Records—relative to disclosure made to the Department of Justice, Executive Department, or Congressional Committees.

• Criminal Investigation Records including all open or closed project files case files, correspondence, activity reports and other material which contains taxpayer data or third party information acquired in connection with a planned, open, or closed case.

• Fraud Referrals—all case files, correspondence, or related documents which contain information regarding items referred to Criminal Investigation.

• Examination Selection Criteria and Formulas. Cycle Variables and Volume Controls.

• Microfilm—all cartridges, cassettes, or other microfilm media which contain taxpayer data or account information.

• Classified Information—Top Secret, Secret, or Classified high security items must be stored using methods identified in Exhibit 1.

3. *Normal Security*—All tax data or Privacy Act information which has *not* been identified as requiring High Security or Special Protection, which contains taxpayer, Privacy Act, or other protected information.

Exhibit 1 should be used as a graphic aid in determining alternate methods of safeguarding protected items. Available methods of protection include the use of secured perimeter or area space and or containerization.

Locks

The lock is the most accepted and widely used security device for protecting installations and activities, personnel, tax data, classified material and government and personal property. All containers, rooms, buildings, and facilities containing vulnerable or sensitive items should be locked when not in actual use.

However, regardless of their quality or cost, locks should be considered as *delay devices only*, and not complete deterrents. Many ingenious locks have been devised, but equally ingenious means have been developed to open them surreptitiously. Some types of locks require considerable time and expert manipulation for covert opening, but all will succumb to force with the proper tools. Therefore, the locking system must be planned and used in conjunction with other security measures if a high degree of security is to be obtained.

Exhibit 1: Protection Alternative Chart

Protected Item Classification	Perimeter Type	Interior Type	Container Type
Special Protection Items			
SP-1	NA	NA	safe vault
SP-2	NA	NA	security container
SP-3	NA	NA	locked container
High Security Items			
Alternative 1	Secured	NA	locked container
Alternative 2	NA	Secured	NA
Alternative 3	NA	NA	security container/security room
Normal Security Items			
Alternative 1	Secured	NA	NA
Alternative 2	NA	NA	locked container

NA Not Applicable

Types of Locking Devices

Locks that are currently available range from the very simple (and easily defeated) variety through highly developed key locks, to combination locks, and even include the highly sophisticated electronic-coded switches.

The degree of protection afforded by a well-constructed vault, safe, or filing cabinet may be measured in terms of the resistance of the locking mechanism to picking, manipulation, or drilling. Two major types of locking devices are:

Key Locks—The time for picking most standard pin-tumbler locks (including those that are specially keyed) ranges from a few seconds to a few minutes. High-security key locks are also vulnerable to surreptitious defeat; however, such defeat is much more difficult. In most cases, a special tool is devised for opening a particular lock. The possibility of the loss and compromise of a key and the possibility of a duplicate being made should also be considered in determining the security value of a key-type lock. Keys should be issued only to persons having a need to have access to an area, room, or container. The number of duplicates should be kept to a minimum. The key issued to an individual will be kept with the individual and not left in desk drawers or other unsecure places.

A Custody Receipt should be used to record the issuance of all keys.

Someone should be responsible for periodically reviewing and reconciling all key and combination records.

Combination Locks—This popular type of lock is incorporated in padlocks, vaults, and doors. Combination locks have several advantages over key locks. First, a combination lock may have many possible combinations, effectively eliminating the possibility of opening the lock by dialing all possible combinations. Second, there is no key which can be lost or compromised. Finally, and most important, modern versions of the combination lock are highly resistant to all forms of undetected attack because no direct access to the lock mechanism itself is required for normal operation. There are several different types of combination locks offering varying degrees of protection. The best types are the "manipulation resistant" locks. The locks meeting requirements of FSS Specification FF-P-110, are considered the most suitable for securing lock bar filing cabinets and similar containers.

Inspection and Maintenance Procedures for Locks

A periodic inspection by the Security Officer should be made on all locks to determine the locking mechanism's effectiveness, to detect tampering, and to make replacements. This may be accomplished by inserting a "test key" (any comparable key other than the assigned key) no more than one-quarter inch into keyway. Turn test key by hand, using the normal amount of force required to open lock. If the lock opens during inspection it should be replaced immediately.

Periodic preventive maintenance of locks should be performed to ensure adequate lubrication, rust prevention on outer surfaces, and cleaning of dust and moisture from keyways. Combination locks must also be serviced (cleaned and greased). By periodic servicing, the life of a combination lock can be greatly extended.

Control and Safeguarding of Keys and Combinations

Access to a locked area, room, or container can only be controlled if the key or combination is controlled. As soon as the combination is obtained by an unauthorized person or otherwise compromised or the key is lost, the security provided by that particular lock is lost.

The combination to each lock will be changed:

- when the safe or lock is originally received,
- at least once each year,
- when an employee who knows the combination retires, terminates employment, or transfers to another office job, or
- whenever the combination is compromised in some other way.

Combinations should be given only to those who have a need to have access to the area, room, or container. Combinations should not be written on calendar pads, desk blotters, or any other item even though it is carried on one's person or hidden away. A record of combinations should be maintained.

Combinations for other than safes and vaults, and accountability records for container keys, should be maintained by the management. These records should include an inventory of total keys available for each container.

Envelopes containing combinations should be placed in a container with the same or a higher security classification as the highest classification of the material authorized for storage in the container or area the lock secures.

One key to all space, properly identified as to the door(s) it will open, should be maintained in a central location.

Locking Systems for Secured Areas

Minimum requirements for locking systems for Secured Areas are as follows:

1. High Security pin-tumbler cylinder locks which meet the following requirements must be used to secure doors to Secured Areas after normal duty hours.

- Key-operated mortised or rim-mounted dead bolt lock.
- Have a dead bolt throw of one inch or longer.
- Be of double cylinder design. Cylinders are to have five or more pintumblers.
- If bolt is visible when locked, it must contain hardened inserts or be made of steel.
- Both the key and the lock must be "Off Master." Convenience type locking devices such as card keys, sequenced button activated locks used in conjunction with electric strikes, etc., are authorized for use only during duty hours.

2. All locks and keys to secured areas should be numbered with an unrelated number system.

3. Keys to secured areas not in the personal custody of an authorized employee, and any combinations, should be stored in a security container with a 3 position combination lock.

4. The number of keys or knowledge of the combination to a secured area should be kept to the absolute minimum. Keys and combinations should be given only to those individuals, preferably supervisors, who have a frequent need to access the area after duty-hours.

Padlocks should be locked to the staple or hasp, or placed inside the container, when the area or container is open, to preclude theft, loss, or substitution of the padlock.

Security Container—To maintain the integrity (preserve the rating) of the security container (lateral), two keys and only two keys should be available for each lock. If the central core of a security container lock is replaced with a non-security lock which has more than two keys, then the container would not qualify as a security container.

A recent development is the magnetic padlock which uses a magnetic key. The key is operated by placing the key on the side of the lock and not by inserting the key into the lock. This lock is not authorized for use within the Internal Revenue Service.

Automatic Detection Equipment

There is a variety of automatic detection equipment. These include, but are not limited to, door and window contacts, motion detectors, sound detectors, photo electric beams, pressure plates, window tapes, vibration sensors, and pressure switches. These are all designed to set off an alarm at a given location when the sensor is disturbed.

Care must be taken in selecting the right equipment to meet the requirement. In any case, the installation must comply with Underwriters' Laboratories, Inc., Standards for Safety 681, Installation No. 1, except that walls, floors, and ceilings need not be protected.

All alarms should annunciate at a protection console, a central station, or local police station where a timely response is available.

Security During Office Moves

When it is necessary for an office to move to another location, plans must be made to properly protect and account for all tax data and other information, as well as government property. Careful consideration must be given to the circumstances of the move, the distance involved and the method to be used in making the move. Tax documents and other information will be in locked cabinets or sealed packing cartons while in transit. Accountability will be maintained to ensure that cabinets or cartons do not become misplaced or lost during the move. IRS material will remain in the custody of an agency employee and accountability will be maintained throughout the move.

Handling, Transmission, and Disposition of Tax and Tax Related Information

Handling

The handling of tax and tax-related documents must be such that the documents do not become misplaced, or available to unauthorized personnel. Only those employees who have a need to know will be permitted access to tax and tax-related information.

Transmission

Any time tax information is transmitted from one location to another, care must be taken to provide safeguards. In the event the material is hand-carried by an individual in connection with a trip or in the course of daily activities, it must be kept with the individual. If it becomes necessary to leave the material in an automobile, it must be locked in the trunk with the rest of the car locked, and then left for only a short period. Hotel and motel rooms are usually not good locations to secure tax information.

All shipments of tax returns and return information (including magnetic media and microfilm) will be documented on a transmittal, and monitored to ensure that each shipment is properly and timely received and acknowledged.

Federal returns and return information may be obtained by Federal, state and local agencies only to the extent the information is needed for, and is reasonably expected to actually be used for, an authorized statutory purpose.

Any agency which receives returns or return information for an authorized use may not use the returns or information in any manner or for any purpose not consistent with that authorized use. (If an agency may receive the information for a different authorized use under a different provision of IRC 6103, a separate request under that separate provision is necessary.) An unauthorized secondary use is specifically prohibited and may result in discontinuation of disclosures to the agency and in the imposition of civil or criminal penalties on the responsible officials.

Returns and return information will be disclosed to an agency only to the extent the agency can reasonably expect it will actually use the information for an authorized purpose. An agency's records of the information it requests should include some record of the result of using the information or of why the information was not used. If an agency receiving information on a continuing basis finds it is receiving information which, for any reason, it is unable to utilize, it should contact the IRS official responsible for liaison with respect to the continuing disclosure and modify the request.

In any case, IRS will disclose Federal returns and return information only to the extent that an agency satisfactorily establishes that the requested information can reasonably be expected to actually be used for an authorized purpose.

IRS will evaluate "need and use" in all safeguard reviews.

XVIII. Disposal of Tax Information Upon Completion of Use

The Tax Reform Act of 1976 requires that certain actions be taken by users of Federal tax information upon completion of use of the information in order to protect its confidentiality.

Agency officials and employees will either return the information (including any copies made) to the office from which it was originally obtained or make the information undisclosable and include in the agency's annual report a description of the procedures utilized.

The following precautions should be observed when Federal tax information is destroyed:

- Material furnished to the user and user generated material such as extra copies, photoimpressions, computer printouts, carbon paper, notes, stenographic notes and work papers should be destroyed by burning, mulching, pulping, shredding, disintegrating, or handcutting.

- Burning precautions: The material is to be either burned in an incinerator that produces enough heat to burn the entire bundle or the bundle should be separated to insure that all pages are consumed.

- Shredding precautions: To make reconstruction more difficult, the paper should be inserted so that lines of print are perpendicular to the cutting line; small amounts of shredded paper should not be allowed to accumulate in the shredder bin. The paper should be shredded to effect 5/16-inch wide or smaller strips, microfilm should be shredded to effect a 1/35-inch strip.

- Pulping should be accomplished in such a manner that all material is reduced to particles one inch or smaller.

- Disintegrating should be accomplished with a ½-inch or smaller screen.

Federal tax data in identifiable form must never be released to private contractors for unsupervised destruction. Destruction of the data should be witnessed by an agency employee in a manner sufficient to safeguard the data from unauthorized disclosure.

After it has served its purpose, magnetic tape containing Federal tax data must not be made available for reuse by other offices or released for destruction without first being subjected to electromagnetic erasing. If reuse is not intended, the tape should be destroyed by cutting into lengths of 18 inches or less or by burning to effect complete incineration.

Whenever disk media leaves the physical or systemic control of the agency for maintenance, exchange or other servicing, any Federal tax information on it must first be destroyed as provided below. If reuse is not practical, the information recorded on the disc will be destroyed by:

- Completely overwriting all data tracks a minimum of three times, using maximum current that will not damage or impair the recording equipment; or

- Running a magnetic strip, of sufficient length to reach all areas of the disc over and under each surface a minimum of three times.

If the information cannot be destroyed as indicated, the disc will be damaged in an obvious manner to prevent use in any disc drive unit and discarded.

The safeguard requirements cease to apply to any return or return information to the extent that they are disclosed in the course of any judicial or administrative proceeding and to the extent that they are made a part of the public record thereof.

XIX. Reporting Indications of Improper Disclosure

Upon discovery of a possible improper disclosure of Federal tax information by a Federal employee, a State employee, or any other person, the individual making the observation or receiving information should contact the office of the appropriate Internal Revenue Service Regional Inspector.

State and local agencies which are Exchange Subscribers to the FTS circuit may call all telephone numbers listed below (except those with single asterisks) by using their FTS access code and dialing the appropriate seven digit telephone number.

All other State and local agencies can call the telephone numbers listed below (except those with double asterisks) by using the commercial telephone circuits and dialing the area code and seven digit number.

Region	Regional Office	States Served by the Region	Telephone Number
Southeast	Atlanta	Georgia, Alabama, South Carolina, North Carolina, Mississippi, Florida, Tennessee, Arkansas, Louisiana	(404) 455-2770* 231-2770**
Western	San Francisco	Alaska, Idaho, Hawaii, California, Oregon, Nevada, Washington	(415) 974-7200* 454-7200*
Mid-Atlantic	Philadelphia	Maryland, New Jersey, Pennsylvania, Virginia, Delaware, District of Columbia	(215) 597-0928
Midwest	Chicago	North Dakota, South Dakota Illinois, Iowa, Wisconsin, Nebraska, Missouri, Minnesota, Montana	(312) 886-5820
Southwest	Dallas	New Mexico, Texas, Wyoming, Colorado, Oklahoma, Kansas, Utah, Arizona	(214) 767-5035* 729-5035**
North Atlantic	New York	New York, Maine, Massachusetts, Vermont, Connecticut, New Hampshire, Rhode Island	(212) 264-9130
Central	Cincinnati	Ohio, Michigan, Indiana, Kentucky, West Virginia	(513) 684-3562
Foreign Operations District (Mid-Atlantic Region)	Philadelphia	Commonwealth of Puerto Rico, Virgin Islands, Guam, American Samoa, Commonwealth of Northern Mariana Islands, & Trust Territory of the Pacific Islands	(215) 597-0928

*Commercial Telephone Circuit Only.
**FTS Telephone Circuit Only.

XX. IRS Safeguard Reviews

IRS conducts on-site reviews of agencies' safeguards at least once every five years. Generally reviews of State and local agencies and Federal agencies outside of the Washington, DC area are conducted by IRS District Disclosure and Security personnel. Reviews of Federal agencies headquartered in the Washington, DC area are conducted by the IRS Disclosure and Security Division. State and local agencies receiving return information under provisions of the Deficit Reduction Act will be reviewed periodically by the agency assigned safeguard responsibility in accordance with a schedule established by the responsible agency and approved by IRS or by IRS District Disclosure and Security personnel.

☆ U.S. GOVERNMENT PRINTING OFFICE: 1986 - 491-487 - 814/45036

Department
of the
Treasury
Internal
Revenue
Service

Publication 1075
(Rev. 1-86)